Dept. of Math. University of Oslo
Statistical Research Report No. 4
ISBN 82–553–1351–6 September 2002
ISSN 0806–3842

Reliability Analysis

Encyclopedia of Actuarial Science

Bent Natvig

Department of Mathematics, University of Oslo,

P.O. Box 1053 Blindern, N–0316 Oslo, Norway

e-mail: bent@math.uio.no

In reliability analysis one is interested in studying the reliability of a technological system being small or large. As examples of small systems we have washing machines and cars, whereas tankers, oilrigs and nuclear power plants are examples of large systems, see **marine insurance**, **nuclear risks**. By the reliability of a system we will mean the probability that it functions as intended. It might be tacitly assumed that we consider the system only for a specified period of time (for instance one year) and under specified conditions (for instance disregarding war actions and sabotage). Furthermore, one has to make clear what is meant by functioning. For oilrigs and nuclear power plants it might be to avoid serious accidents, see **accident insurance**, such as a blow-out or a core-melt.

It should be acknowledged that the relevance of reliability theory to insurance was pointed out by Straub [27] at the start of the seventies. In his paper he applies results and techniques from reliability theory to establish bounds for unknown loss

probabilities. A recent paper by Mallor & Omey [14] is in a way in the same spirit. Here the objective is to provide a model for a single component system under repeated stress. Fatigue damage is cumulative, so that repeated or cyclical stress above a critical stress will eventually result in system failure. In the model the system is subject to load cycles (or shocks) with random magnitude $A(i)$ and intershock times $B(i)$, $i = 1, 2, \ldots$ The $(A(i), B(i))$ vectors are assumed independent. However, the authors make the point that another interpretation can be found in insurance mathematics. Here $A(i)$ denotes the claim size of the ith claim, whereas the $B(i)$'s denote interclaim times, see **claim size process**, **claim number process**. In this case, they study the time until the first run of k consecutive critical (e.g. large) claims and the maximum claim size during this time period.

The scope of the present article is quite different from the ones of these papers. We will present reliability analysis in general having the following two main points of view. Reliability analysis is a very helpful tool in **risk assessment** when determining the insurance premiums for risks, especially of **rare events**, associated with large systems consisting of both technological and human components. Furthermore, reliability analysis is relevant in **risk management** of any technological system, the aim now being to say something helpful on how to avoid accidents. This is an area of growing importance representing an enormous challenge for an **insurance company**.

It is a characteristic of systems that they consist of components being put together in a more or less complex way. Assume the system consists of n components

and introduce the following random variables ($i = 1, \ldots, n$)

$$X_i(t) = \begin{cases} 1 & \text{if the } i\text{th component functions at } t \\ 0 & \text{otherwise,} \end{cases}$$

and let $\boldsymbol{X}(t) = (X_1(t), \ldots, X_n(t))$. The state of the system is now uniquely determined from $\boldsymbol{X}(t)$ by

$$\phi(\boldsymbol{X}(t)) = \begin{cases} 1 & \text{if the system functions at } t \\ 0 & \text{otherwise} \end{cases}$$

$\phi(\cdot)$ is called the structure function. Note that it is assumed that both the components and the system are satisfactorily described by binary random variables. Barlow & Proschan [2] is the classical textbook in binary reliability theory. [6] is a nice expository paper on reliability theory and its applications until 1985.

As an illustration consider a main power supply system of a nuclear power plant given in Figure 1.

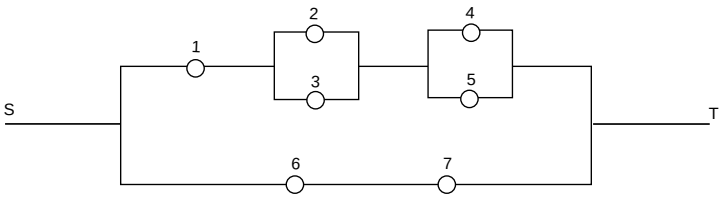

Figure 1. Main power supply system of a nuclear power plant

The system consists of two main branches in parallel providing power supply to the nuclear power plant. The system is working if and only if there is at least one connection between S and T. Component 1 represents offsite power from the grid

whereas component 6 is an onsite emergency diesel generator. Components 2 and 3 are transformers while 4, 5 and 7 are cables (including switches, etc.). It is not too hard to be convinced that the structure function of the system is given by

$$\begin{aligned}\phi(\boldsymbol{X}(t)) = 1 - \big\{1 - X_1(t)[X_2(t) + X_3(t) - X_2(t)X_3(t)] \\ \times [X_4(t) + X_5(t) - X_4(t)X_5(t)]\big\}\{1 - X_6(t)X_7(t)\}\end{aligned} \tag{1}$$

Now let $(i = 1, \ldots, n)$

$$p_i(t) = P(X_i(t) = 1) = E\, X_i(t), \tag{2}$$

which is called the reliability of the ith component at time t. The reliability of the system at time t is similarly given by

$$h_\phi(t) = P(\phi(\boldsymbol{X}(t)) = 1) = E\, \phi(\boldsymbol{X}(t)) \tag{3}$$

If especially $X_1(t), \ldots, X_n(t)$ are stochastically independent, we get by introducing $\boldsymbol{p}(t) = (p_1(t), \ldots, p_n(t))$ that $h_\phi(t) = h_\phi(\boldsymbol{p}(t))$. For this case, for the power supply system of Figure 1, we get from (3), (1), (2)

$$\begin{aligned}h_\phi = 1 - \big\{1 - p_1(t)[p_2(t) + p_3(t) - p_2(t)p_3(t)][p_4(t) + p_5(t) - p_4(t)p_5(t)]\big\} \\ \times \{1 - p_6(t)p_7(t)\}\end{aligned} \tag{4}$$

For large n, efficient approaches are needed such as the technique of recursive disjoint products, see [1]. For network systems the factoring algorithm can be very efficient, see [24].

If $X_1(t), \ldots, X_n(t)$ are stochastically dependent, $h_\phi(t)$ will also depend on how the components function simultaneously. In this case, if only information on $\boldsymbol{p}(t)$ is available, one is just able to obtain upper and lower bounds for $h_\phi(t)$, see [17]. The same is true, if n is very large, even in the case of independent components. Dependencies between component states may for instance be due to a common but dynamic environment, see the expository paper [25] where the effects of the environment are described by a stochastic process.

In reliability analysis it is important not to think of systems just as pure technological ones. Considering the break-down of the Norwegian oilrig Alexander Kielland in 1980, where 123 persons lost their lives, one should be convinced that the systems of interest consist of both technological and human components. The same conclusion is more obvious when considering the accident at the Three Mile Island nuclear power plant in 1979 and even more the Chernobyl **catastrophy** in 1986, see [23]. Until now systems have often been designed such that the technological components are highly reliable, whereas the human components operating and inspecting these are rather unreliable. By making less sophisticated technological components which can be operated and inspected by the human components with high reliability, a substantial improvement of overall system reliability can be achieved. It should, however, be admitted that analysing human components is very different from analysing technological ones, see [28]. Similarly, software reliability is a branch of reliability analysis having special challenges, see [26].

In risk management improving the safety of a system is essential. We then need

measures of the relative importance of each component for system reliability, see [21]. Barlow & Proschan [3] suggested that the most important component is that having the highest probability of finally causing system failure by its own failure. Natvig [19] has developed a theory supporting another measure. Here the component whose failure contributes most to reducing the expected remaining lifetime of the system is the most important one. The latter measure obviously is constructed to improve system life expectancy, whereas the first one is most relevant when considering accidents scenarios. It should be noted that the costs of improving the components are not entering into these measures.

The journal Nature, published an article [16] on an incident coming close to a catastrophy, which occured in 1984 in a French pressurized water reactor at Le Bugey, not far from Geneva. Here it is stated: "But the Le Bugey incident shows that a whole new class of possible events had been ignored – those where electrical systems fail gradually. It shows that risk analysis must not only take into account a yes or no, working or not working, for each item in the reactor, but the possibility of working with a slightly degraded system." This motivates socalled multistate reliability analysis where both the components and the system are described in a more refined way than just as functioning or failing. For the power supply system of Figure 1, the system state could for instance be the number of main branches in parallel functioning. The first attempts of developing a theory in this area came in 1978, see [4], [9]. Further work is reported in [18]. In [20] multistate reliability analysis is applied to an electrical power generation system for two nearby oilrigs.

The amounts of power that may possibly be supplied to the two oilrigs are considered as system states. The type of failure at Le Bugey is also an example of "cascading failures", see the recent paper [12].

The Chernobyl catastrophy provided new data on nuclear power plants. What type of theory do we have to benefit from such data in future risk analyses in the nuclear industry? The characteristic feature of this type of theory is that one benefits both from data for the system's components and for the system itself. Furthermore, due to lack of sufficient data one is completely dependent on benefiting from the experience and judgement of engineers concerning the technological components and on those of psychologists and sociologists for the human components. This leads to subjectivistic probabilities and hence to **Bayesian statistics**. A series of papers on the application of the Bayesian approach in reliability are given in [5]. In [7] hierarchical Bayes procedures are proposed and applied to failure data for emergency diesel generators in U.S. nuclear power plants. A more recent Bayesian paper with applications to preventive system maintenance of interest in **risk management** is [11].

A natural starting point for the Bayesian approach in system reliability is to use expert opinion and experience as to the reliability of the components. This information is then updated by using data on the component level from experiments and accidents. Based on information on the component level, the corresponding uncertainty in system reliability is derived. This uncertainty is modifed by using expert opinion and experience on the system level. Finally, this uncertainty is up-

dated by using data on the system level from experiments and accidents. Mastran & Singpurwalla [15] initiated research in this area in 1978, which was improved in [22]. Recently, ideas on applying Bayesian hierarchical modelling, with accompanying **Markov Chain Monte Carlo methods**, in this area have turned up, see [13].

It should be noted that the use of expert opinions is actually implemented in the regulatory work for the nuclear power plants in the USA, see [8]. A general problem when using expert opinions is the selection of the experts. Asking experts technical questions on the component level as in [10], where the consequences for the overall reliability assessment on the system level are less clear, seems advantageous. Too much experts' influence directly on system level assessments could then be prevented.

Finally, it should be admitted that the following obstacles may arise when carrying through a reliability analysis of a large technological system:

(i) lack of knowledge on the functioning of the system and its components

(ii) lack of relevant data

(iii) lack of knowledge on the reliability of the human components

(iv) lack of knowledge on the quality of computer software

(v) lack of knowledge of dependences between the components

These obstacles may make it very hard to assess the probability of failure in a **risk**

assessment of a large technological system. However, still a **risk management** of the system can be carried through by using reliability analysis to improve the safety of the system.

References

[1] Ball, M.O. & Provan, J.S. (1988). Disjoint products and efficient computation of reliability, *Oper. Res.* **36**, 703–715.

[2] Barlow, R.E. & Proschan, F. (1975). *Statistical Theory of Reliability and Life Testing. Probability Models*. Holt, Rinehart & Winston, New York.

[3] Barlow, R.E. & Proschan, F. (1975). Importance of system components and fault free events, *Stochastic Processes Appl.* **3**, 153–173.

[4] Barlow, R.E. & Wu, A.S. (1978). Coherent systems with multistate components, *Math. Operat. Res.* **4**, 275–281.

[5] Barlow, R.E., Clarotti, C.A. & Spizzichino, F. (1993). *Reliability and Decision Making*. Chapman & Hall, London.

[6] Bergman, Bo. (1985). On reliability theory and its applications (with discussion), *Scand. J. Statist.* **12**, 1–41.

[7] Chen, J. & Singpurwalla, N.D. (1996). The notion of "composite reliability" and its hierarchical Bayes estimator, *J. Amer. Statist. Ass.* **91**, 1474–1484.

[8] Chhibber, S., Apostolakis, G.E. & Okrent, D. (1994). On the use of expert judgements to estimate the pressure increment in the Sequoyah containment at vessel breach, *Nucl. Technol.* **105**, 87–103.

[9] El-Neweihi, E., Proschan, F. & Sethuraman, J. (1978). Multistate coherent systems, *J. Appl. Prob.* **15**, 675–688.

[10] Gåsemyr, J., Natvig, B. (1995). Using expert opinions in Bayesian prediction of component lifetimes in a shock model, *Math. Operat. Res.* **20**, 227–242.

[11] Gåsemyr, J. & Natvig, B. (2001). Bayesian inference based on partial monitoring of components with applications to preventive system maintenance, *Naval Research Logistics* **48**, 551–577.

[12] Lindley, D.V. & Singpurwalla, N.D. (2002). On exchangeable, causal and cascading failures, *Statistical Science* **17**, 209–219.

[13] Lynn, N., Singpurwalla, N.D. & Smith, A. (1998). Bayesian assessment of network reliability. *Siam Review* **40**, 202–227.

[14] Mallor, F. & Omey, E. (2001). Shocks, runs and random sums, *J. Appl. Prob.* **38**, 438–448.

[15] Mastran, D.V. & Singpurwalla, N.D. (1978). A Bayesian estimation of the reliability of coherent structures, *Oper. Res.* **26**, 663–672.

[16] *Nature* (1986). Near-catastrophe at Le Bugey, **321**, 462 (29 May).

[17] Natvig, B. (1980). Improved bounds for the availability and unavailability in a fixed time interval for systems of maintained, interdependent components, *Adv. Appl. Prob.* **12**, 200-221.

[18] Natvig, B. (1985). Multistate coherent systems, *Encyclopedia of Statistical Sciences* **5**, 732–735.

[19] Natvig, B. (1985). New light on measures of importance of system components, *Scand. J. Statist.* **12**, 43–54.

[20] Natvig, B., Sørmo, S., Holen, A.T. & Høgåsen, G. (1986). Multistate reliability theory – a case study, *Adv. Appl. Prob.* **18**, 921–932.

[21] Natvig, B. (1988). Reliability: Importance of components. *Encyclopedia of Statistical Sciences* **8**, 17–20.

[22] Natvig, B. & Eide, H. (1987). Bayesian estimation of system reliability, *Scand. J. Statist.* **14**, 319–327.

[23] Natvig, B. & Gåsemyr, J. (1996). On probabilistic risk analysis of technological systems, *Radiation Protection Dosimetry* **68**, 185–190.

[24] Satyanarayana, A. & Chang, M.K. (1983). Network reliability and the factoring theorem, *Networks* **13**, 107–120.

[25] Singpurwalla, N.D. (1995). Survival in dynamic environments. *Statistical Science* **10**, 86–103.

[26] Singpurwalla, N.D. & Wilson, S.P. (1999). *Statistical Methods in Software Engineering*. Springer, New York.

[27] Straub, E. (1971/72). Application of reliability theory to insurance. *Astin Bull.* **6**, 97–107.

[28] Swain, A.D. (1990). Human reliability analysis: need, status, trends and limitations, *Reliab. Eng. Syst. Saf.* **29**, 301–313.

B. NATVIG